



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,158	07/22/2003	Jeffrey S. Bardsley	5577-264	7454
20792 7590 12/20/2006 MYERS BIGEL SIBLEY & SAJOVEC PO BOX 37428 RALEIGH, NC 27627			EXAMINER TOLENTINO, RODERICK	
			ART UNIT 2134	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		12/20/2006	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/624,158	<b>Applicant(s)</b> BARDSLEY ET AL.	
	<b>Examiner</b> Roderick Tolentino	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 22 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 07/22/2003.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1 – 22 are pending.

#### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 – 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flowers et al. U.S. Patent No. (7,073,198) in view of Dahlstrom et al. U.S. PG-Publication No. (2004/0006704).

4. As per claims 1, 11 and 21, Flowers teaches establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV) (Flowers, Col. 4 Lines 26 – 37) but fails to teach receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

However, in an analogous art Dahlstrom teaches a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type (Dahlstrom, Paragraph 0006) and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat (Dahlstrom, Paragraph 0042).

At the time the invention was made, it would have been obvious to use Dahlstrom's system for determining security vulnerabilities with Flowers' method for detecting vulnerability in a network because it offers the advantage of properly having ways to fix detected vulnerabilities.

5. As per claims 2 and 12, Flowers as modified teaches comprises receiving a TMV history file in response to installation, configuration or maintenance of the computer system (Dahlstrom, Paragraph 0018) and wherein the processing comprises processing countermeasures that are identified in the TMV history file (Dahlstrom, Paragraph 0006, record of fixes).

6. As per claims 3 and 13, Flowers as modified teaches updating a threat management information base for the computer system to account for the countermeasures that are processed file (Dahlstrom, Paragraphs 0027 and 0036).

Art Unit: 2134

7. As per claims 4, 14 and 22, Flowers as modified teaches determining whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat (Flowers, Col. 4 Lines 26 – 37) adding at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat (Flowers, Col. 4 Lines 26 – 37) and processing countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system (Dahlstrom, Paragraph 0042).

8. As per claims 5 and 15, Flowers as modified teaches the processing comprises installing and running the countermeasure (Dahlstrom, Paragraphs 0044 and 0042).

9. As per claims 6 and 16, Flowers as modified teaches wherein the receiving comprises receiving a TMV including therein the first field that provides identification of at least one operating system type that is affected by a computer security threat, the second field that provides identification of an operating system release level for the operating system type, a fourth field that provides identification of at least one application program type that is affected by the computer security threat and a fifth field that provides identification of a release level for the application program type, the third field providing identification of a set of possible countermeasures for the application program type and the application program release level (Flowers, Col. 4 Lines 26 – 37,

identifies OS) and wherein the processing comprises processing countermeasures that are identified in the TMV if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat (Dahlstrom, Paragraph 0042, fixes).

10. As per claims 7 and 17, Flowers as modified teaches determining whether the TMV identifies the application program type and application programming release level for the computer system as being affected by the computer security threat (Flowers, Col. 4 Lines 26 – 37, identifies OS), adding at least one instance identifier to the TMV to account for multiple instances of the application program running on the computer system if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat (Flowers, Col. 4 Lines 26 – 37) and processing countermeasures that are identified in the TMV for the instance of the application program type and application program release level when the instance of the application program type and application program release level is instantiated in the computer system (Dahlstrom, Paragraph 0042).

11. As per claims 8 and 18, Flowers as modified teaches the set of possible countermeasures comprises an identification of a countermeasure mode of installation (Dahlstrom, Paragraphs 0044 and 0042).

12. As per claims 9 and 19, Flowers as modified teaches the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures (Dahlstrom, Paragraph 0027).

Art Unit: 2134

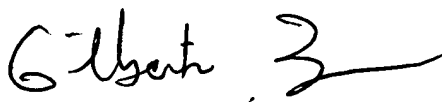
13. As per claims 10 and 20, Flowers as modified teaches the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures (Dahlstrom, Paragraph 0042).

**Conclusion**

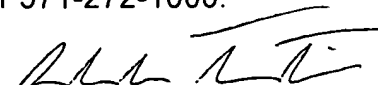
14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



Roderick Tolentino  
Examiner  
Art Unit 2134